The modern vehicular system has a large number of microcontrollers which control functions like air bags, ABS, Driver Drowsiness Detection (DDD), infotainment, and many more. These applications require security measures against malicious manipulation. As well, to cater to the run-time controllability of these systems, the application code and data size has increased manifold.

The article here talks about various methods for implementing security architectures which can prevent hacking of the code and data stored in on-chip flash memory of SoCs and microcontrollers.

**Conventional architecture of flash controller**

Flash memory in a SoC generally consists of a flash memory controller and a flash memory array module. The flash memory controller provides control functions and acts as an interface between the system bus and the flash memory array.

**Enhanced flash architecture for security**

The conventional flash memory controller can be modified in following ways to provide security for the flash memory array.

**a) Secure access through password comparison**

Normal read, write/program and erase accesses can be changed to secure access by implementing a password comparison mechanism. A bus-master is allowed to access the flash array only if the input password, matches with the stored password. The stored password can be kept in a One-Time-Programmable and read protected region in a Non-Volatile memory like flash or a Read Only Memory (ROM) or fuse. Only the flash controller can access this secured memory when a password comparison is initiated by a master.

**b) Partitioning flash memory array into secure and non-secure regions**

Flash memory array can be partitioned into secured and non-secured regions. The secured region
can be used to store critical data. Non-secured flash partitions can be mapped to the main interface. And the secured flash partitions can be mapped to the alternate interface.

Flash controller can route the trusted masters to the alternate interface, and thereby allow them to access secured region.

c) Intelligent arbiter in flash controller

Flash controllers can contain an arbitration logic whose main function is to provide arbitration among the masters when they are accessing the flash memory simultaneously. So every master must possess a unique master identification number to help the flash controller to differentiate between the masters. The Master ID can be used to differentiate between trusted and non-trusted master. Hence a non-trusted master accessing the part of flash, which is meant only for a trusted master, can be restricted by the controller.

Conclusion

To ensure the reliability of the vehicle, it has become extremely important to ensure that code resides in a secured memory region to avoid malfunctioning of the system. Security has become a key driving factor for the automotive industry, for supplier and OEM to meet the stringent safety requirements. The architectures here present ways in which data security in an SoC can be achieved.

References

- ISO 26262
- Freescale Security Technology
- Automotive Security: From Standards to Implementation
- Safety & security architecture for automotive ICs